I would like to express my opposition to requirements that law enforcement agencies be able to tap all VoIP communications. This is for three major reasons:

1. Expense. VoIP's main future is not in allowing people to communicate via computer to people on the standard telephone network, but in standardizing voice communications between computers, at which point given the parties' having internet connections will mean unlimited communications at no additional expense -- so long as those computers communicate point-to-point. One of the requirements of the regulation is that these "wiretaps" must be performed indetectably; if most communications are performed point-to-point, but a tapped connection involved additional communication or routing through another point, then those taps would be detectable. This means that in order to fulfill the indetectability requirement, ALL connections would need to be routed through central servers, which would involve a significant expense where no such servers would be needed. It would also insert communications delays which users would find undesirable.

2. Ineffectiveness. Once VoIP were standardized, you would start seeing new communications systems springing up, designed to operate in parallel, and immune to any wiretap on the VoIP system, establishing direct connections that would bypass the routing through servers noted above.

3. Lack of necessity. While a tap on a VoIP line might be expensive and/or ineffective, it would be assumed that law enforcement would be tapping the INTERNET CONNECTIONS of suspects. Such a tap could be used to read VoIP communications as well, and a system of avoiding a tap on the VoIP system iteself would be unable to avoid a tap on the actual connection.

Given all of this, I would have to opine that the only real effect of a VoIP tap requirement would be the placement of a drag on the technology.